CLAIMS

1. A method comprising:

encrypting data that is stored in memory other than a video card memory;

transferring the encrypted data over a bus to the video card;

decrypting the encrypted data on the video card, said decrypting taking place independent of a graphics processor unit (GPU) on the card needing to process the encrypted data; and

storing decrypted data in the video card memory.

2. The method of claim 1, wherein the act of decrypting is performed automatically whenever encrypted data is transferred to the video card.

3. The method of claim 1, wherein the act of storing comprises storing the decrypted data in protected portions of the video memory.

4. The method of claim 1, wherein the act of decrypting is performed by a memory controller on the video card.

5. The method of claim 1 further comprising ensuring that video memory portions have a compatible degree of protection when unencrypted data is to be transferred between different video memory portions on the video card.

6. The method of claim 1, wherein the act of decrypting comprises decrypting the encrypted data using a decryption key that is associated with a memory portion into which the unencrypted data is to be stored.

7. One or more computer-readable media having computer-readable instructions thereon which, when executed by one or more processors, cause the one or more processors to:

encrypt data that is stored in memory other than a video card memory;

transfer the encrypted data over a bus to the video card;

decrypt the encrypted data on the video card independent of a graphics processor unit (GPU) on the card needing to process the encrypted data; and

store decrypted data in the video card memory.

8. The one or more computer-readable media of claim 7, wherein the instructions cause the one or more processors to decrypt the encrypted data automatically whenever encrypted data is transferred to the video card.

9. A method comprising:

providing unencrypted data in a video card memory;

encrypting the unencrypted data on the video card; and

transferring the encrypted data off of the video card.

10. The method of claim 9, wherein the act of providing comprises providing the unencrypted data into a video memory portion that is protected.

11. The method of claim 10, wherein the memory portion is protected with an access control list.

12. The method of claim 9, wherein the act of providing comprises providing the unencrypted data into a video memory portion having an associated encryption/decryption key pair that can be used to respectively encrypt and decrypt the data provided in said video memory portion.

13. The method of claim 9, wherein the act of encrypting is performed any time the unencrypted data is to be provided into system memory off of the video card.

14. The method of claim 9, wherein the act of encrypting is performed any time the unencrypted data is to be provided onto a bus connected between the video card and a computer system's central processor unit, the video card comprising part of the computer system.

15. One or more computer-readable media having computer-readable instructions thereon which, when executed by one or more processors, cause the one or more processors to:

provide unencrypted data in a video card memory;

encrypt the unencrypted data on the video card any time the unencrypted data is to be provided onto a bus between a computer system's memory off of the video card; and

transfer the encrypted data onto the bus.

16. A video card comprising:

a graphics processor unit (GPU) for processing data that is to be rendered on a monitor;

memory operably associated with the graphics processor unit for holding data that is to be or has been processed by the GPU;

a display converter for converting digital data to signals for use in rendering the data on the monitor; and

a memory controller configured to receive encrypted data and decrypt the encrypted data into protected regions of the memory.

17. The video card of claim 16, wherein the memory controller is configured to ensure that unencrypted data transfers on the video card are made between protected memory regions.

18. The video card of claim 17, wherein the memory controller is configured to ensure that protected memory regions have a compatible degree of protection.

19. The video card of claim 18, wherein the memory controller determines compatibility, based at least in part, on access control lists that are associated with individual protected memory regions.

20. The video card of claim 18, wherein the memory controller determines compatibility, based at least in part, on one or more encryption keys associated with individual protected memory regions.

21. The video card of claim 16 further comprising a key manager for controlling one or more encryption/decryption key pairs that are used to respectively encrypt and decrypt data on the video card.

22. The video card of claim 21, wherein the key manager comprises an individual integrated circuit chip.

23. The video card of claim 21, wherein the key manager is communicatively linked with the memory controller and is configured to program the memory controller for encrypting and decrypting data on the video card.

24. The video card of claim 16, wherein the memory controller is configured to encrypt unencrypted data that is stored in a protected region of the memory on the video card so that the encrypted data can be moved to an unprotected region of the memory on the video card.

25. The video card of claim 24 further comprising a decryptor operably associated with the memory on the video card and configured to receive encrypted data from the memory and decrypt the encrypted data so that the decrypted data can be provided to the display converter for processing.

26. The video card of claim 25 further comprising a key manager for controlling one or more encryption/decryption key pairs that are used to respectively encrypt and decrypt data on the video card, the key manager being configured to instruct the decryptor on which key to use to decrypt encrypted data.

27. The video card of claim 16, wherein the memory controller comprises a memory protection table having one or more table entries, individual table entries associating at least one encryption/decryption key pair with a memory region that is to hold data that can be encrypted and decrypted using the key pair associated with the memory region.

28. The video card of claim 16, wherein the memory controller comprises one or more access control lists, individual access control lists being associated with individual regions of the memory and defining which entities can access a particular memory region.

29. A method comprising:

providing a graphics processor unit (GPU) on a video card for processing data that is to be rendered on a monitor;

providing memory on the video card operably associated with the GPU for holding data that is to be or has been processed by the GPU;

providing a display converter for converting digital data to signals for use in rendering the data on the monitor; and

providing a memory controller configured to receive encrypted data and decrypt the encrypted data into protected regions of the memory.

30. The method of claim 29, wherein the memory controller is provided to ensure that unencrypted data transfers on the video card are made between protected memory regions.

31. The method of claim 30, wherein the memory controller ensures that protected memory regions have a compatible degree of protection.

32. The method of claim 31, wherein compatibility is determined by the memory controller, based at least in part, by access control lists that are associated with individual protected regions.

33. The method of claim 31, wherein compatibility is determined by the memory controller, based at least in part, on one or more encryption keys associated with individual protected regions.

34. The method of claim 29 further comprising providing a key manager on the video card for controlling one or more encryption/decryption key pairs that are used to respectively encrypt and decrypt data on the video card.

35. The method of claim 34, wherein the act of providing the key manager comprises providing an integrated circuit chip.

36. The method of claim 34, wherein the act of providing the key manager comprises communicatively linking the key manager with the memory controller so that the key manager can program the memory controller for encrypting and decrypting data on the video card.

37. The method of claim 29, wherein the providing of the memory controller comprises providing a memory controller that is configured to encrypt unencrypted data that is stored in a protected region of the memory on the video card so that the encrypted data can be moved to an unprotected region of the memory on the video card.

38. The method of claim 37 further comprising providing a decryptor operably associated with the memory on the video card and configured to receive encrypted data from the memory and decrypt the encrypted data so that the decrypted data can be provided to the display converter for processing.

39. The method of claim 38 further comprising providing a key manager for controlling one or more encryption/decryption key pairs that are used to respectively encrypt and decrypt data on the video card, the key manager being configured to instruct the decryptor on which key to use to decrypt encrypted data.

40. The method of claim 29, wherein providing of the memory controller comprises providing a memory controller comprising a memory protection table having one or more table entries, individual table entries associating at least one encryption/decryption key pair with a memory region that is to hold data that can be encrypted and decrypted using the key pair associated with the memory region.

41. The method of claim 29, wherein providing of the memory controller comprises providing a memory controller comprising one or more access control lists, individual access control lists being associated with individual regions of the memory and defining which entities can access a particular memory region.

42. A method comprising:

providing one or more key pairs, individual key pairs comprising an encryption key that can be used to encrypt data and a decryption key that can be used to decrypt data encrypted with the encryption key; and

associating individual key pairs with individual portions of memory that comprise part of a video card memory.

43. The method of claim 42, wherein said acts of providing and associating are performed on a video card.

44. The method of claim 42, wherein said act of associating comprises defining a table on the video card, the table having individual entries that associate individual key pairs with individual portions of the memory.

45. The method of claim 44, wherein the table is defined as part of a memory controller on the video card.

46. The method of claim 42 further comprising using an encryption key to encrypt data that is stored in an associated portion of the memory.

47. The method of claim 46, wherein the act of using is performed prior to transferring the data off of the video card.

48. The method of claim 46, wherein the act of using is performed prior to transferring the data to an unprotected portion of the memory on the video card.

49. The method of claim 42 further comprising using a decryption key to decrypt encrypted data that has been received over a bus external to the video card.

50. The method of claim 49 further comprising providing the decrypted data into a portion of the memory associated with the decryption key that was used to decrypt the encrypted data.

51. A method comprising:

providing data into a first portion of memory on a video card, the first portion of the memory having a first level of protection;

operating on the data to provide resultant data on the video card;

determining whether a second portion of the memory on the video card has a level of protection that is compatible with the first level of protection; and

if the first and second levels of protection are compatible, providing the resultant data into the second portion of the memory on the video card.

52. The method of claim 51, wherein protection levels are defined, at least in part, by encryption keys associated with the first and second memory portions.

53. The method of claim 51, wherein protection levels are defined, at least in part, by access control lists associated with the first and second memory portions.

54. The method of claim 51, wherein the act of operating is performed by a graphics processor unit comprising part of the video card.

55. The method of claim 51, wherein the resultant data is different from the data that was provided into the first portion of the memory on the video card.

56. A method comprising:

reading data from one or more portions of memory on a video card, individual portions of the memory having an associated encryption/decryption key pair;

recording key pairs associated with the memory portions from which the data was read;

operating on the data read from the one or more portions of the memory to provide output data;

ascertaining whether the key pairs associated with the memory portions from which the data was read are equivalent to a key pair associated with a video memory portion that is to serve as a destination for the output data; and

if the key pairs are equivalent, providing the output data into the destination video memory portion.

57. A method comprising:

encrypting data that is stored in memory other than a video card memory;

transferring the encrypted data over a bus to the video card;

placing the encrypted data into an unprotected portion of memory on the video card;

decrypting the encrypted data on the video card; and

placing the decrypted data into a protected portion of memory on the video card.

58. The method of claim 57, wherein the act of decrypting is performed by a graphics processor unit on the video card.

59. The method of claim 57 further comprising programming a graphics processor unit on the video card with decryption capabilities sufficient to enable the graphic processor unit to decrypt encrypted data that resides in the unprotected memory portion of the video card.

60. The method of claim 59, wherein the act of programming is performed by a key manager on the video card, the key manager being configured to manage one or more encryption/decryption keys.

61. The method of claim 60, wherein the key manager comprises an integrated circuit chip.

62. The method of claim 57 further comprising protecting protected portions of the memory on the video card using a memory controller.

63. The method of claim 62, wherein the act of protecting is performed using, at least in part, one or more access control lists that define the protection for the protected portions of the video memory.

64. The method of claim 62, wherein the act of protecting comprises ensuring that protected video memory portions have a compatible degree of protection when unencrypted data is to be transferred between different protected video memory portions on the video card.

65. The method of claim 57 further comprising after said act of placing:

operating on the data in the protected portion of the video memory to provide resultant data;

encrypting the resultant data; and

placing the encrypted resultant data in a protected portion of the video memory.

66. The method of claim 65, wherein said acts of encrypting the resultant data and placing the resultant data are performed, at least in part, by a graphic processor unit on the video card.

67. The method of claim 66 further comprising:

decrypting the encrypted resultant data using a decryptor on the video card; and

after said decrypting of the encrypted resultant data, providing the decrypted resultant data to a display converter for further processing.

68. A video card comprising:

a graphics processor unit (GPU) for processing data that is to be rendered on a monitor, the GPU comprising encryption and decryption functionality sufficient to encrypt and decrypt data on the video card;

memory operably associated with the GPU for holding data that is to be or has been processed by the GPU, the memory comprising protected and unprotected portions;

a display converter for converting digital data to analog signals for use in rendering the data on the monitor; and

a memory controller configured to protect the protected portions of the video memory.

69. The video card of claim 68, wherein the memory controller comprises one or more access control lists that are utilized to protect the protected portions of the memory.

70. The video card of claim 69, wherein the access control lists define entities that can access the protected portions of the video memory.

71. The video card of claim 68 further comprising a key manager on the video card configured to program the GPU with the encryption/decryption functionality.

72. The video card of claim 68, wherein the GPU is configured to decrypt data in unprotected portions of the memory into protected portions of the memory.

73. The video card of claim 68, wherein the GPU is configured to encrypt data in protected portions of the memory into unprotected portions of the memory.

74. A method comprising:

providing a graphics processor unit (GPU) on a video card for processing data that is to be rendered on a monitor, the GPU comprising encryption and decryption functionality sufficient to encrypt and decrypt data on the video card;

providing memory, on the video card, operably associated with the GPU for holding data that is to be or has been processed by the GPU, the memory comprising protected and unprotected portions;

providing, on the video card, a display converter for converting digital data to signals for use in rendering the data on the monitor; and

providing, on the video card, a memory controller configured to protect the protected portions of the video memory.

75. The method of claim 74, wherein providing the memory controller comprises providing a memory controller comprising one or more access control lists that are utilized to protect the protected portions of the memory.

76. The method of claim 75, wherein the access control lists define entities that can access the protected portions of the video memory.

77. The method of claim 74 further comprising providing a key manager on the video card configured to program the GPU with the encryption/decryption functionality.

78. The method of claim 74, wherein providing the GPU comprises providing a GPU configured to decrypt data in unprotected portions of the memory into protected portions of the memory.

79. The method of claim 74, wherein providing the GPU comprises providing a GPU configured to encrypt data in protected portions of the memory into unprotected portions of the memory.

80. A method comprising:

receiving, into unprotected memory portions of a video card, encrypted data that is intended to be processed by a graphic processor unit (GPU) on the card;

decrypting the encrypted data into protected memory portions of video card; and

encrypting unencrypted data in protected memory portions of the video card into protected memory portions of the video card.

81. The method of claim 80, wherein the acts of encrypting and decrypting are performed by the GPU.

82. The method of claim 80, wherein protected memory portions are protected by a memory controller using one or more access control lists that define which entities can access the protected memory portions.

83. The method of claim 80 further comprising encrypting data on the video card any time the data is to be provided off of the video card and onto a bus connected with a computer system's central processor unit (CPU).

84. The method of claim 80 further comprising encrypting data on the video card any time the data is to be provided off of the video card and onto a bus connected with a computer system's memory.